Detect Unauthorized Access to Cloud Secrets Management Stores, Detection Strategy DET0130

Archived: 2026-04-05 18:28:08 UTC

AN0366

Detection of suspicious access to cloud-native secret management systems (AWS Secrets Manager, GCP Secret Manager, Azure Key Vault, HashiCorp Vault). Focuses on abnormal secret retrieval activity, such as secrets being accessed by unusual identities, from unexpected regions, outside business hours, or at high volume. Correlates API calls to secret retrieval with surrounding authentication events, role assumptions, and anomalous execution patterns.

Log Sources

Mutable Elements

Field	Description
PrivilegedRoles	Set of accounts or roles allowed to retrieve secrets; deviations may indicate misuse.
TimeWindow	Temporal window to correlate secret access with authentication and anomalous context.
AccessPatterns	Expected frequency and volume of secret retrievals per user/service; anomalies may indicate exfiltration.
RegionConstraints	Regions in which secret access is expected; access from unusual geographies may indicate compromise.